OBLON, SPIVAK, ET AL DOCKET #: 240264US6 INV: Hideo SATO SHEET 1 OF 12

1/12

FIG. 1A

ELLIPTIC-CURVE-CRYPTOSYSTEM PROCESSING CIRCUIT

REGISTERS

ELLIPTIC-CURVE-OPERATION CORE CIRCUIT

FIG. 1B

SHA-1 PROCESSING CIRCUIT

REGISTERS

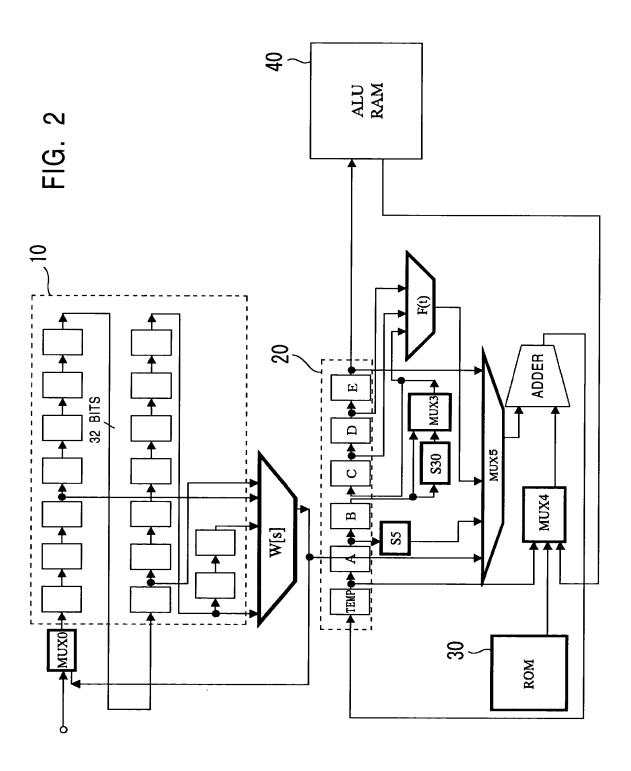
SHA-1 OPERATION CORE CIRCUIT

FIG. 1C

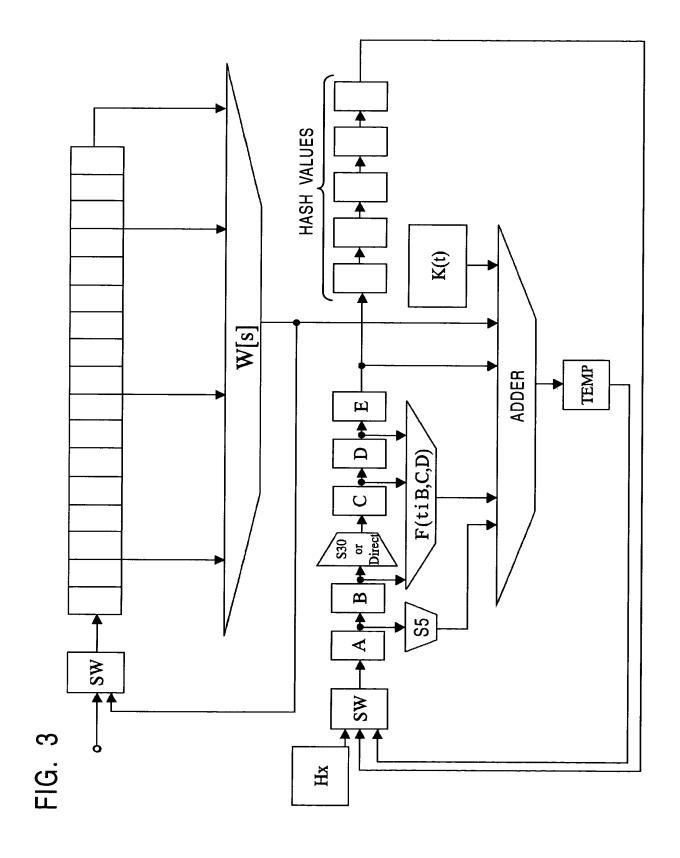
REGISTERS

ELLIPTIC-CURVE-OPERATION CORE CIRCUIT SHA-1 OPERATION CORE CIRCUIT

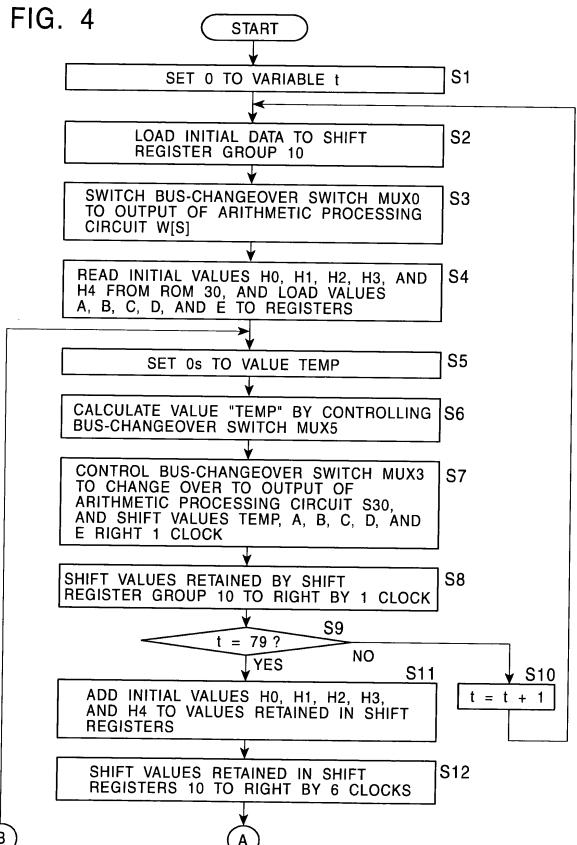
2/12



3/12

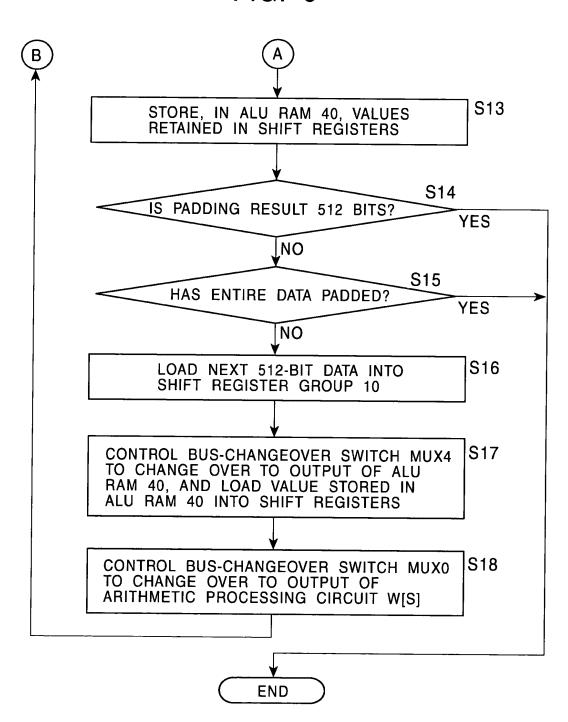


4/12

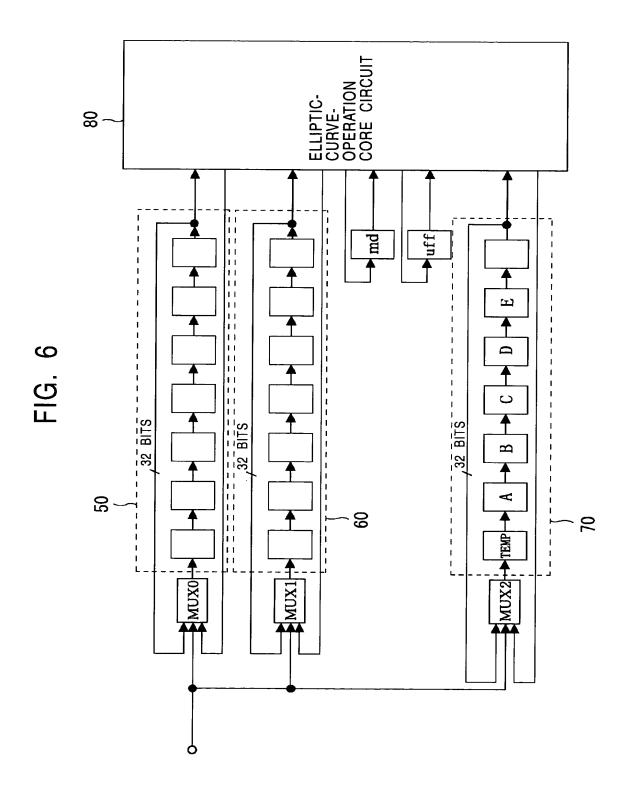


5 / 12

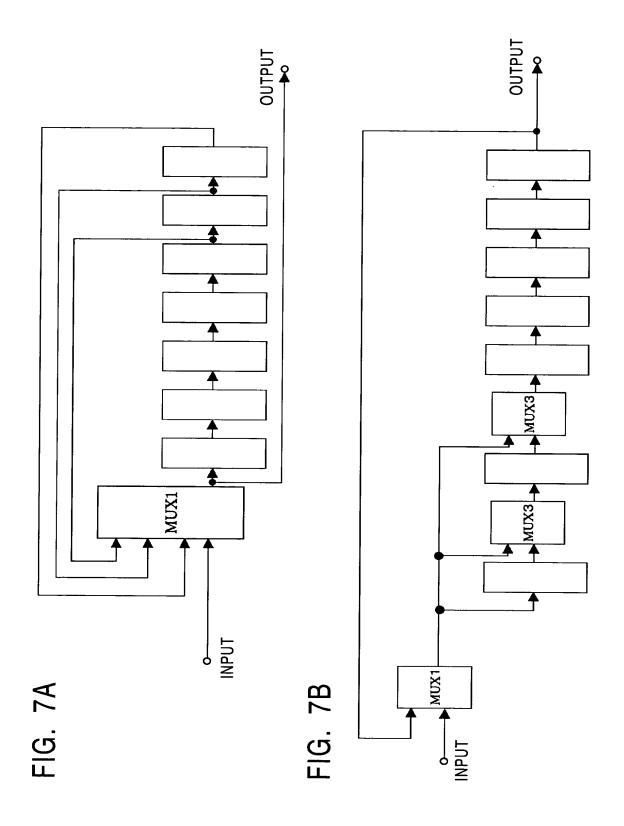
FIG. 5



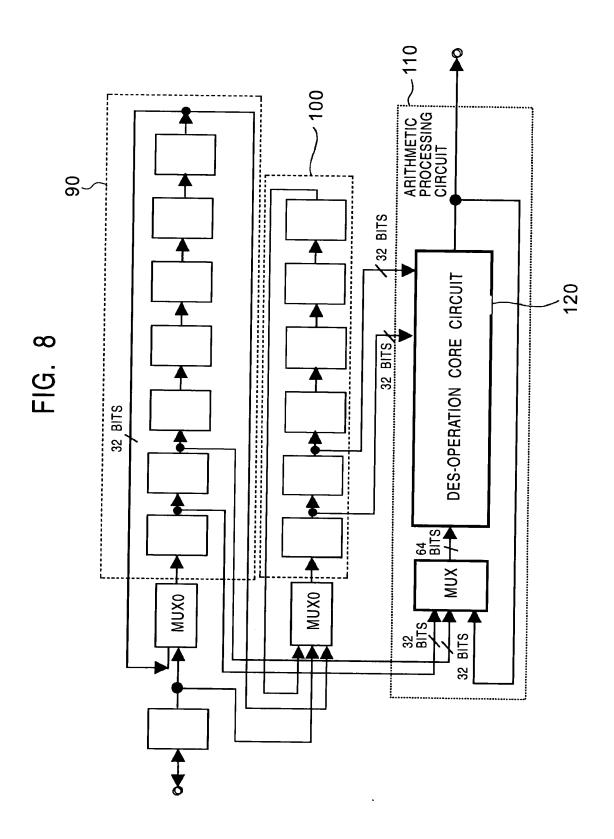
6 / 12



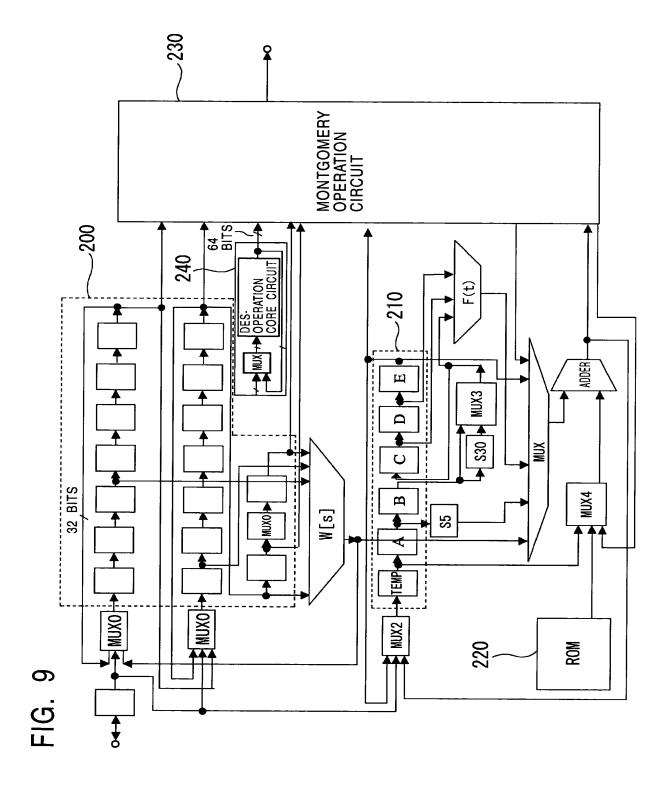
7 / 12



8 / 12

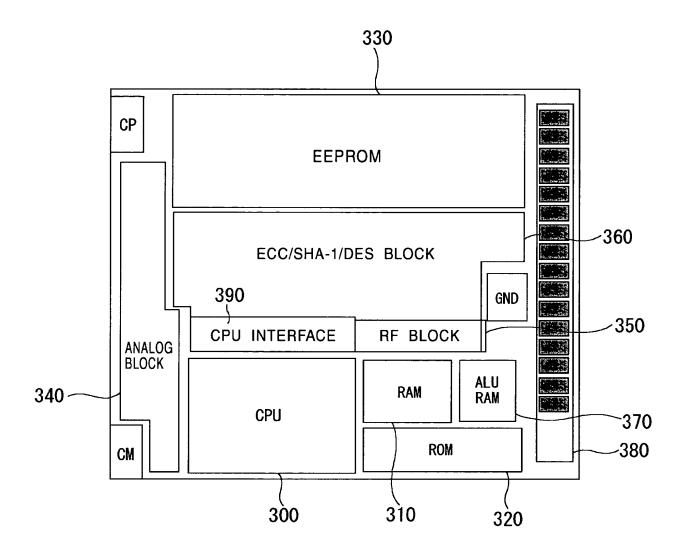


9/12

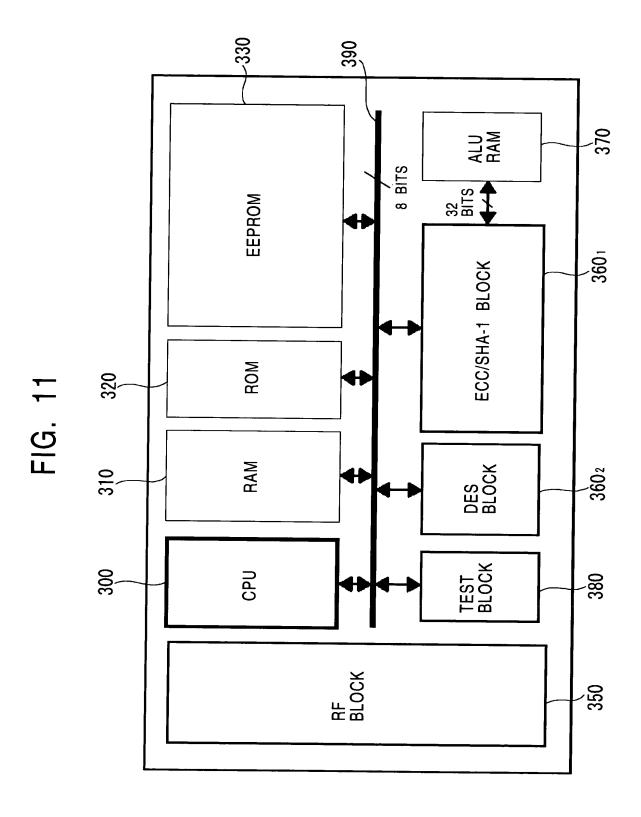


10 / 12

FIG. 10



11 / 12



12 / 12

